Model Question Paper

Code: 23CC5T02 / 23CC5O01 **R23**

SWARNANDHRA COLLEGE OF ENGINEERING & TECHNOLOGY
[AUTONOMOUS]
Seetharampuram, NARSAPUR-534 280
B. Tech V Semester Regular Examinations

INTRODUCTION TO CYBER SECURITY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

(CYBER SECURITY)

(Common for Open Elective -I)

Note: 1. The question paper consists of two parts (**Part-A and Part-B**)
2. Answer all questions from **Part-A**
3. Answer all questions from **Part-B** with either or choice

Duration: 3 Hours **Max Marks: 70**

PART-A (5x2=10M)

S No		Question	Cognitive Level	CO	Marks
1	a	Define "Compromised Computer" and give an example.	K1	1	2
	b	List any two safe internet usage practices.	K1	1	2
	c	What is meant by "Fair Use" in Cyber Law?	K1	2	2
	d	Define SQL Injection and mention one preventive measure.	K2	3	2
	e	Expand CIA in Cyber Security and explain each component in brief.	K1	5	2

PART – B (5X12 = 60 M)

S. No		Question	Cognitive Level	CO	Marks
2	a	Explain "Information Security Best Practices" for securing computer networks	K2	1	6
	b	Discuss privacy guidelines and safe internet usage with real-time examples.	K2	1	6
OR					
3	a	What are compromised computers? Explain different causes and impacts.	K2	1	6
	b	Explain secure communications in networking with suitable examples.	K3	1	6
4	a	Discuss privacy, intellectual property, and professional ethics in cyber security.	K2	2	6
	b	Explain ethical hacking and internet fraud with relevant case studies.	K3	2	6
OR					

5	a	Write short notes on trademarks, electronic evidence, and cybercrimes	K1	2	6
	b	Describe the role of cyber laws in India with examples of important cases.	K2	2	6
6	a	Define penetration testing and explain its types.	K1	3	6
	b	Discuss the process of defining web application test scope with examples.	K3	3	6
		OR			
7	a	List and explain common web architectures from a penetration tester's view.	K2	3	6
	b	Explain different types of web vulnerabilities in detail.	K2	3	6
8	a	Explain SQL injection, XSS, and CSRF with examples and prevention measures.	K2	4	6
	b	Write about forensic technologies and digital evidence collection.	K2	4	6
		OR			
9	a	Discuss SSL, CAPTCHA, and session hijacking in web applications.	K2	4	6
	b	Explain the process of evidentiary reporting and outsider threat protection	K3	4	6
10	a	Explain asset evaluation, business impact analysis, and risk identification	K2	5	6
	b	Discuss the phases of cyber incident response: preparation, detection, containment, eradication, and recovery	K3	5	6
		OR			
11	a	Describe the CIA triangle and its importance in cyber security.	K1	5	4
	b	Write about the phases of incident response with examples.	K2	5	8

Prepared by **Verified by** **Approved By**